FortiOS™ Handbook - FortiGate Connector for Cisco ACI

Version 1.0.32

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Thursday, October 15, 2015

FortiConnector for Cisco ACI - Administration Guide

01-540-293514-20150929

TABLE OF CONTENTS

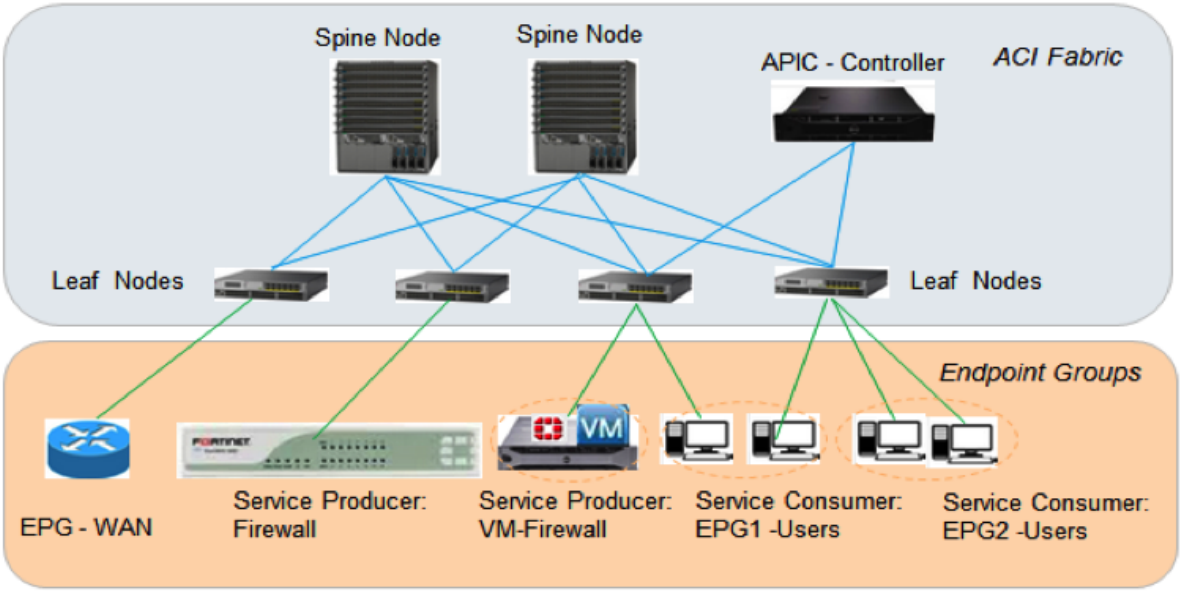
Change Log

Date	Change Description
2015-10-13	Initial Release

Overview

FortiGate Connector for Cisco ACI (Application Centric Infrastructure) is the Fortinet solution to provide seamless integration between Fortinet Firewall (Fortigate) deployment with Cisco APIC (Application Policy Infrastructure Controller). This integration allows customers to perform single point of Fortigate configuration and Management operation through Cisco APIC.

While the FortiGate series of firewalls enable superb firewall services, in a data center environment, the insertion, configuration, and management of network services such as firewall can be quite complex and potentially error-prone tasks. One solution for such data center problems is Cisco's ACI. Cisco's ACI is a policy-based framework with integration of software and hardware in the underlying leaf-spine fabric. In Cisco ACI, the APIC is a tool used to automate service insertion and provisioning into the fabric of the network environment. Network service appliances, both physical and virtual, can be attached to ACI fabric's leaf node through APIC. Traffic demanding certain network services is steered by APIC-managed policies to the appropriate resources. The FortiGate Connector allows FortiGates to be included amongst the list of resources that traffic can be directed to.



Licensing

FortiGate Connector for Cisco ACI is free of charge for Fortinet customers. You need to make sure that you register your FortiGate with FortiCare on support.fortinet.com.

Terms and concepts

FortiGate VDOMs

VDOM or Virtual Domain refers to a discretely administered segment on a FortiGate firewall. A FortiGate firewall that is not segmented and where a single administrator can access all of the firewall is operating in the “root” VDOM. However, it is possible to segment the FortiGate so that different administrators can access different areas of the FortiGate. Credentials for VDOM X will allow access to the resources and settings of VDOM A but no other. There will also be global resources and settings that will require credentials to the root VDOM. When setting up connectivity between Cisco APIC and the FortiGates it will be important to know which VDOMs control the needed resources.

FortiOS RESTful API

REST (sometimes spelled ReST) stands for Representational State Transfer. It is a software architectural style for the WWW. REST systems typically communication over HTTP, using HTTP verbs or commands to retrieve and send information to remote servers.

A good resource for the finer details of Fortinet’s implementation of ReST can be found at http://docs.fortinet.com/uploaded/files/1276/FortiAuthenticator_REST_API_Solution_Guide.pdf

North/South and East/West Traffic

The cardinal compass direction terms to describe traffic flow are used to differentiate between traffic within the cloud or data center and traffic going in and out of the cloud or data center.

- North/South - traffic either heading into or out of a cloud or data center.
- East/West - traffic that is between nodes inside the same cloud or data center.

Features

There are a number of features associated with firewalls in general and FortiGate firewalls in particular. This section should explain which of these features are available through the FortiGate Connector and which are not.

Supported Features

The FortiGate Connector for Cisco ACI supports the following functions:

- Cisco ACI service insertion - software package for FortiGate device deployed to Cisco APIC, containing FortiGate models, function description, version, credentials, as a L4-L7 service.
- Enable tenant configuration to add/modify/delete L4-L7 device of FortiGate firewall service.
- Enable FortiGate deployment as both physical and virtual device (FortiGate chassis & VM).
- Support both transparent (GoThrough) and L3 (GoTo) device mode .
- Automatically create VDOM (context). One VDOM per logical device under a tenant.
- Enable FortiGate specific interface configuration: physical interface and port channel.
- Support IP address configuration on Layer 3 interfaces.
- Support subnet, service and schedule object configuration.
- Enable FortiGate firewall device to connect to endpoint groups (EPGs).
- Support IPv4 policies: match, action, network operations & security features selection (although the Enable/Disable Security profile option in policies is not supported).
- Support NAT.
- Enable service graph to add/modify/delete FortiGate firewall service node.

Unsupported Features

The following features normally found on FortiGates are not supported through the FortiGate Connector for Cisco ACI.

- Security Profiles (Web filtering, etc)
- DoS Policy
- Proxy Policy
- SSL/SSH Inspection
- FortiGate WAN load balance link.
- HA/cluster support.
- Administrator profile for limited access of different administrator accounts.
- Static and dynamic routing except OSPF.
- Firewall port forwarding (destination NAT).
- Firewall logging: allowed traffic, security events, all sessions, etc.
- Firewall packet capture.

- Firewall with FortiGuard DDNS.
- Other Firewall features not specifically listed as supported.

The following information resources are available on the FortiGates but do not integrate with APIC:

- Error Logs
- Statistics Reporting

The unsupported features on APIC may still be used on FortiGate outside of the APIC control; the user must login to FortiGate to configure, monitor, and debug. However, any conflict with the operations from APIC may cause malfunction.

Planned for future releases

FortiGate Connector for Cisco ACI plans to incorporate the following features and functions into future versions of the software:

- Support for OSPF-based routing configuration in the L3 (GoTo) mode from APIC.
- Monitor FortiGate devices (health) status.
- Provide FortiGate device statistics – device and service counters per context.
- Support for logging and error reporting of FortiGate as a L4-L7 device.
- Performance reporting: control and management plane based on APIC, data path on FortiGate.

New features are not limited to this list. These are just the features currently planned for.

Supported Fortinet Products

The supported Fortinet products refers to those that are compatible with the FortiGate Connector for Cisco ACI software, and will properly integrate into the Cisco ACI. The products are separated into models and firmware but it is an “and” set of parameters. In order to be supported the Fortinet product has to be one of the listed models running supported firmware.

Models

FortiGate Connector for Cisco ACI v1.0 supports integration with the following predefined models:

- FG-1000D
- FG-1500D
- FG-3700D
- FG-VM
- Unknown (to be added based on customer's request)

Firmware Versions

FortiGate Connector for Cisco ACI version 1 is compatible with the following FortiOS firmware:

- FortiOS 5.4 (including the Beta version)

Prerequisites

Cisco Side

Before the FortiGate Connector for Cisco ACI can be successfully deployed, a number of prerequisites need to be satisfied within the Cisco environment.

One of the following Cisco ACI environments needs to be in place:

- Cisco ACI v1.1(2h)
- Cisco ACI v1.1(3f)

Within the Cisco ACI, the following configurations need to be completed before Layer 4 -7 Services (in this case, the FortiGate Connector) can be deployed:

- Creation of Access Policies configuration under Fabric menu
- Creation of any need Tenant(s)
- Creation of Network(s) (including Bridge Domain)
- Creation of Application Profile(s)
- Creation of End Point Group(s)
- Creation of Contract(s)

For detail, please consult Cisco APIC deployment Guide.

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/L4-L7_Services_Deployment/guide/b_L4L7_Deploy.html

FortiGate Side

Before the FortiGate Connector for Cisco ACI can be successfully deployed, a number of prerequisites need to be satisfied on the FortiGate side of the equation.

Physical Firewall

1. Configure administrator user name and password.
2. Enable http/https on mgmt. port.
3. Configure IP address in mgmt. port.
4. Enable VDOM-Admin globally.
5. Configure Port-Group if needed.

VM Firewall

1. Assign network ports before start VM
2. Configure administrator user name and password.
3. Enable http/https on mgmt. port.

4. Configure IP address in mgmt. Ports
5. Enable VDOM-Admin globally

Components of the Device Package

To add a network service to ACI fabric, the service's device package needs to be uploaded to APIC. The device package is a zip file containing these components:

Device model or specification

The Device Specification is an XML file called `DeviceModel.xml` that covers descriptions of FortiGate devices, interfaces, connectivity and services. The file contains a hierarchical description of FortiGate devices, including:

- Device functions
- Parameters of each function
- Interfaces/network connectivity information of each function.

Device script

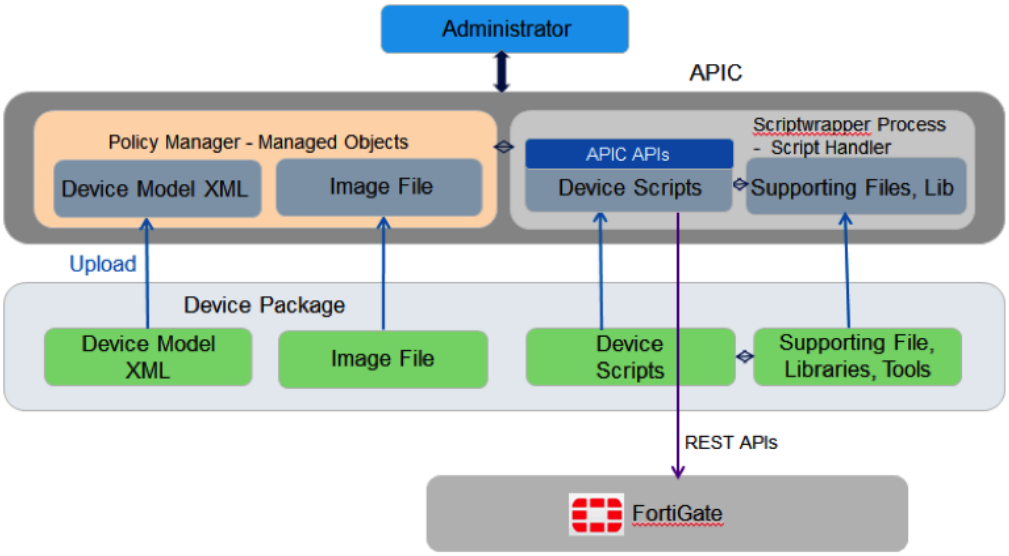
This is a Python file, `DeviceScript.py` with API functions to interface between the Cisco APIC and the FortiGate REST APIs. This Python file is associated by the DeviceModel.xml device specification to device script for APIC.

Directory of supporting files

This component contains supporting Python files, text files and libraries of scripts and tools.

Image file or directory

The directory contains file(s) such as a Fortinet icon (`Fortinet_name.gif`) to be displayed on the APIC management page.



Operational modes

There are two types of network service devices which Cisco APIC integrates with. These types of devices are defined by their operation mode. They are either Go Through or Go To. Normally a device has to be preconfigured as one of these types before its imported package is managed by the APIC.

Go Through Mode (Layer 2)

Devices in Go Through mode are considered layer 2 devices (from the OSI model) and are sometimes known as transparent. They are referred to as transparent because while the traffic goes through them and can be affected by them, they are not seen by the network and are not a destination in their own right for the traffic. They do not route traffic. These devices are not referred to by the packet's destination MAC or IP address. In most cases, these devices will only have an address for the purposes of management.

Go To Mode (Layer 3)

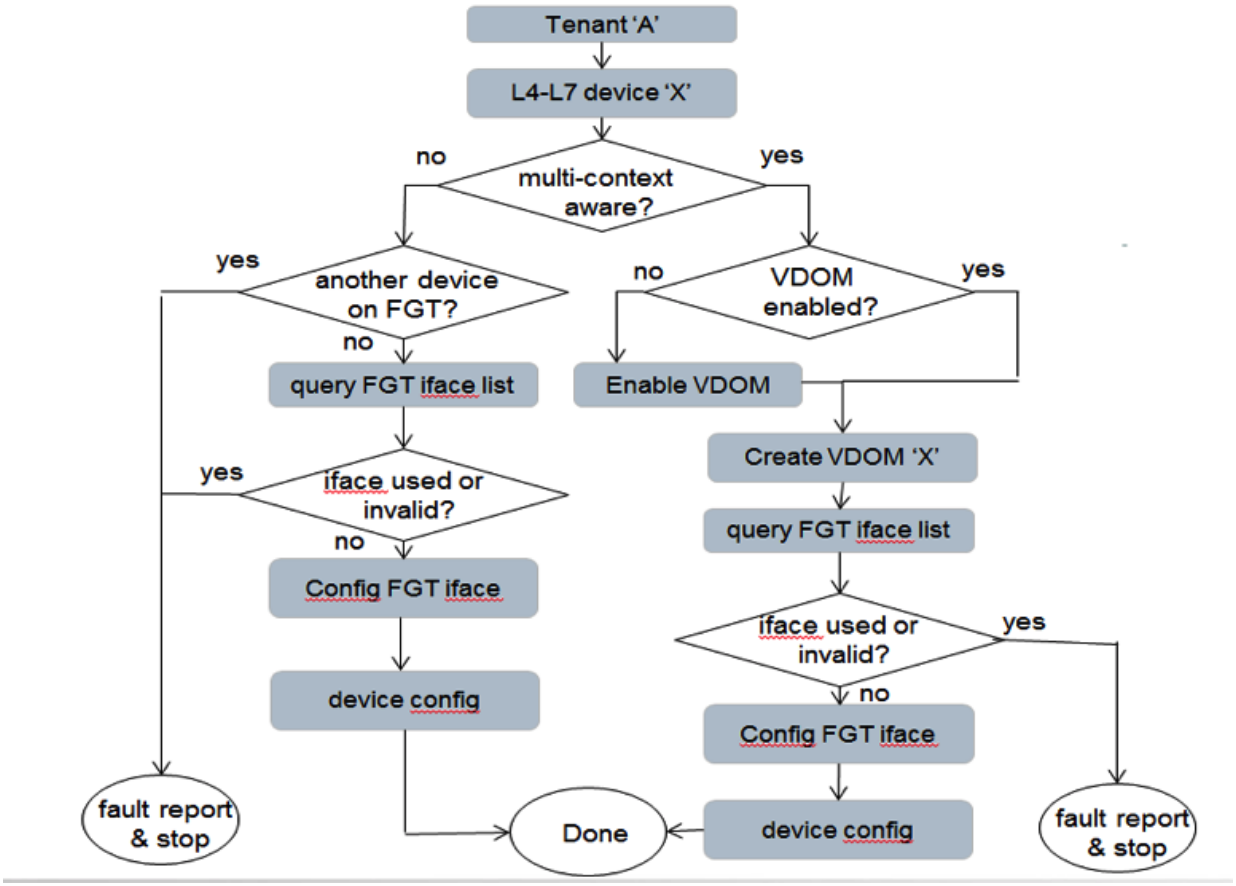
Devices in Go To mode are considered Layer 3 (from the OSI model) devices. They can route traffic and they are referenced as the destination in a packet's destination MAC address or destination IP address.

Multi-tenant multi-device support

Multi-tenant Multi-device is typical in the use cases of this project. The support is worth more detailed description. When FortiGate device is added a tenant's L4-L7 services, multi-context aware can be enabled. This indicates to the device package that the L4-L7 device is going to be a virtual device that shares resources with other tenants on the FortiGate. In FortiGate implementation, this virtual device is represented by a VDOM. Under each tenant, multiple such virtual devices can be configured.

- VDOM name is the device name. One VDOM per device. One or more devices per tenant.
- Each tenant sees all available interfaces and can share interfaces (ports) with other tenants, if it is multi-context aware. Limitation question: To be confirmed – For Physical Device under L3 Routed(GoTo) Mode, Tenant can share physical interface as vlan is used to isolate the physical interface. In VM Device, this is not true. You can only use dedicated VNIC.
- Each FortiGate device supports only a pair of ports. Another pair requires another device added under the tenant.

When the L4-L7 service is deployed to the FortiGate device, the following logic is performed. For simplicity in the first release, the user may need to enable VDOM during FortiGate pre-configuration.



Supported use scenarios

Physical Fortigate

Go-Through Mode for west-east traffic within data center in ACI.

Scenario: Web server and back-end database servers have same subnet in data center; customer needs firewall service between web server and back-end database servers.

Go-To Mode for north-south traffic for Web Server to access DataBase server in data center.

Scenario: Firewall service for Web Server to access DataBase server in data center.

Virtual Fortigate

Go-Through Mode for west-east traffic within data center in ACI.

Scenario: Web server and back-end database servers have same subnet in data center; customer needs firewall service between web server and back-end database servers.

Go-To Mode for north-south traffic for Web Server to access DataBase server in data center.

Scenario: Firewall service for Web Server to access DataBase server in data center.

Installation

To successfully deploy Fortigate Connector into Cisco APIC, customers need to perform the following steps:

• Import Device Package

• Add L4-L7 Device

• Create Functional Profile

• Create Service Graph Template

• Deploy Service Graph Template.

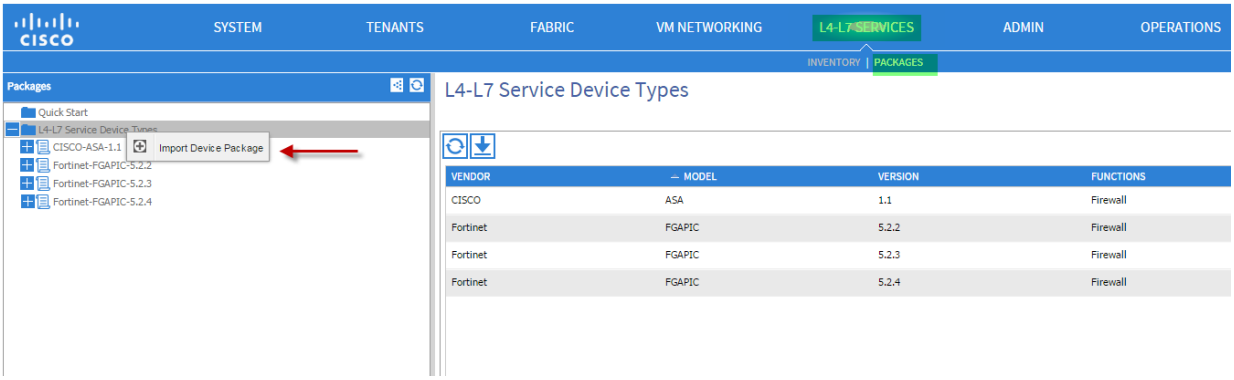
According to the APIC deployment guide, a service device introduces a Layer 4 to Layer 7 service by this typical procedure:

1. Import the device package of the service device,
2. Configure a tenant who asks for network services,
3. Register the device and its logical interfaces,
4. Configure logical device parameters,
5. Configure a layer 3 network,
6. Configure a bridge domain,
7. Configure an application profile,
8. Configure a physical domain (or VMM domain),
9. Configure a VLAN pool,
10. Configure a contract
11. Configure a management endpoint group (EPG),
12. Configure a service graph template,
13. Select default service graph template parameters,
14. Attach the service graph template to a contract
15. Configure additional configuration parameters.

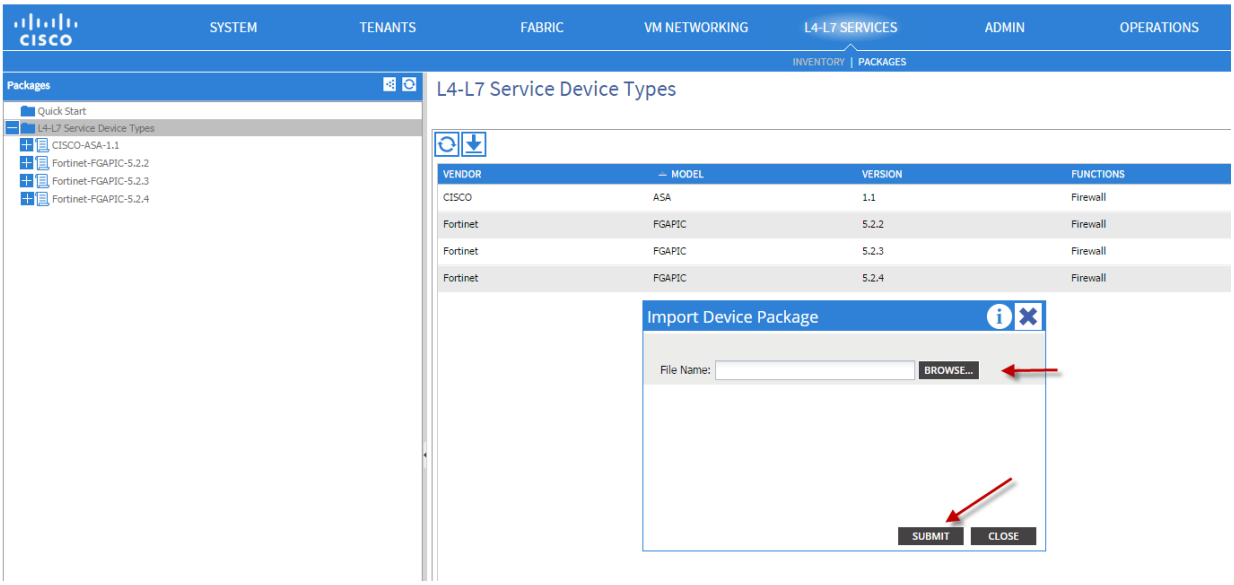
To add a support of a non-Cisco firewall device in the Cisco ACI fabric based data center, a device package should be developed for the APIC. Then the remaining task is standard APIC deployment of a network service device.

Importing the Device Package

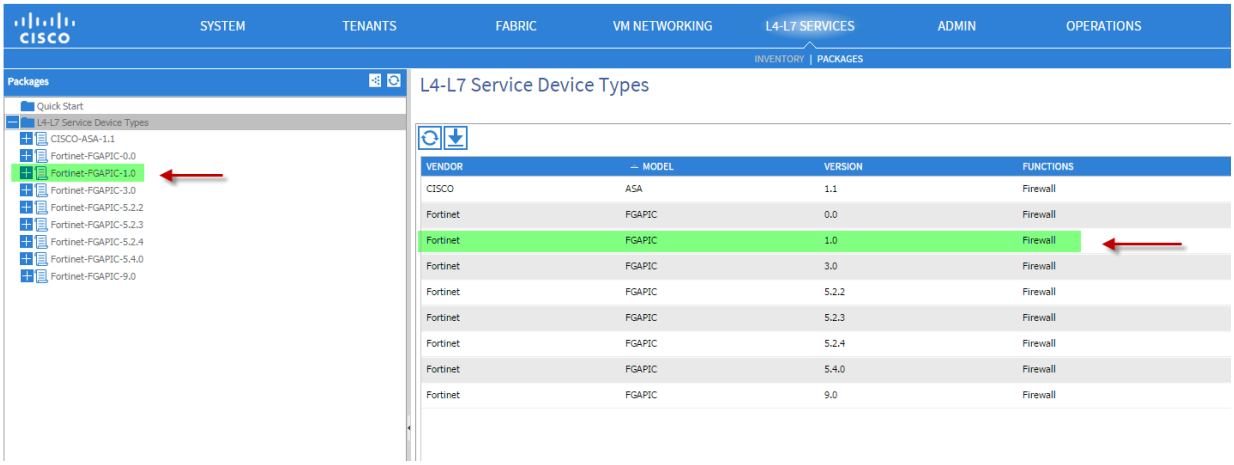
1. Download Device Connector Package from Fortinet Support Web (URL) site to local storage.
2. From APIC menu, Navigate to ***L4-L7 Services > Packages*** and right click on ***L4-L7 Device Type*** on the left hand panel. Select ***Import Device Package***



3. Browse device package from local disk or share device and hit submit.

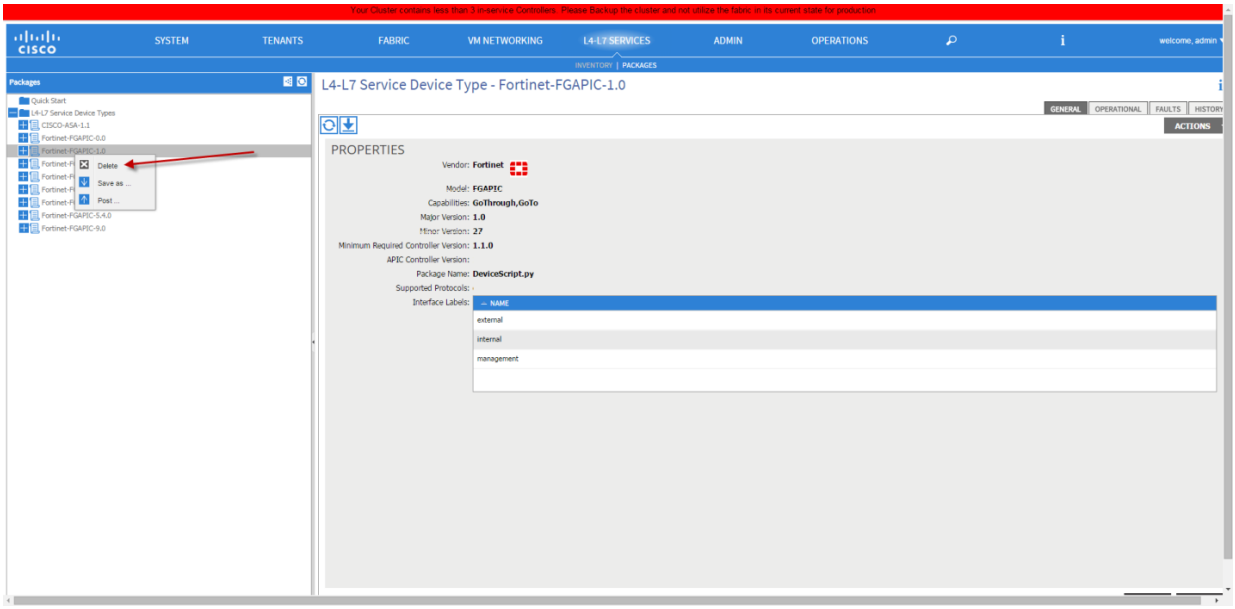


4. Device package should display on the left hand panel.



Remove Device Package

To remove Device Package, navigate to ***L4-L7 Services > Packages*** and right click on the Device package on the left panel and select ***Delete*** option.



Add L4-L7 Device

Within Tenant, Expand ***L4-L7 Services > L4-L7 Devices***, right click on mouse and select "***Create L4-L7 devices***"

GENERAL

Field	Description / Options
Name	Name of the Device
Device Package	Select Device Package from drop down list
Model	• FG-VM • FG-1000D • FG-1500D • FG-3700D • Unknown

Field	Description / Options
Mode	• Single Node / HA Cluster We only support Single Node for current release
Function Type	• GoThrough (L2) • Goto (L3)

CONNECTIVITY

Field	Description / Options
Physical Domain or VMM Domain	Select from drop down list Domain which you should have configured during APIC Access Policies setup
APIC to Device	• Out-of-Band • In-Band

CREDENTIALS

Field	Description
Username	<login name to the Fortigate>
Password	<Password to login to Fortigate>
Confirm Password	<Password to login to Fortigate>

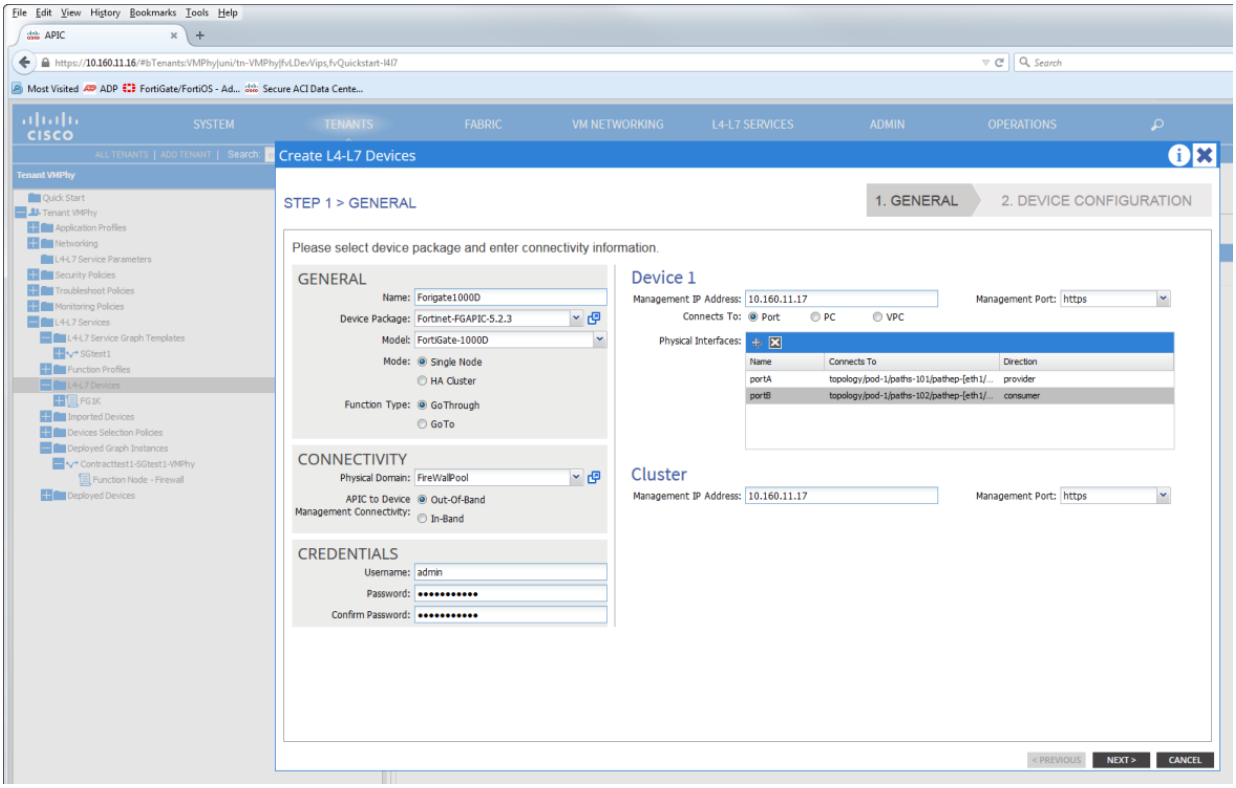
Device 1

Field	Description / Options
Management IP Address	<IP address to connect to Fortigate>
Management Port	• http • https https is the prefer method
Connects To	• Port (Default), PC, VPC
Physical Interfaces	Click on “+” sign to add interfaces connecting from APIC to FortiGate

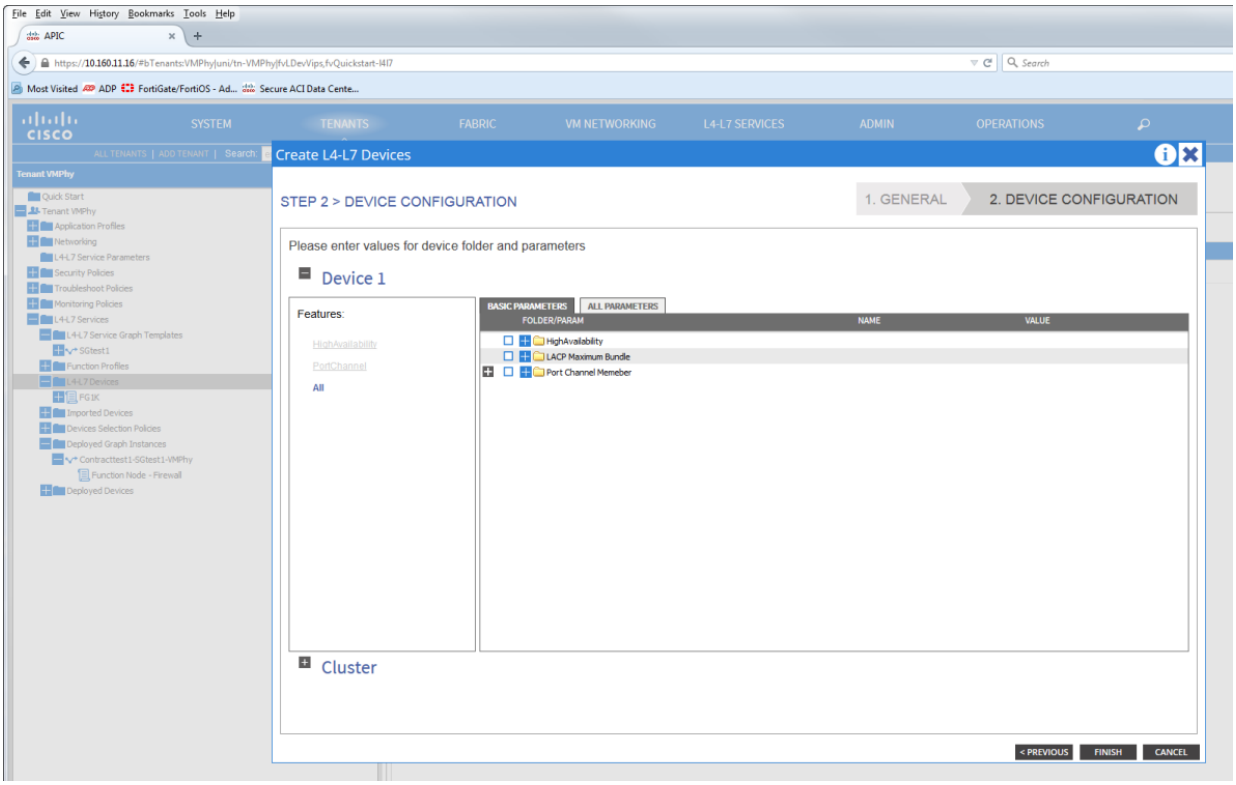
Field	Description / Options
Name	Select from Drop down list to select port. (If using Port Channel, please type in the correct Port Channel name ex:PO1, PO2..etc.)
Connects To	Interface that connects to the APIC
Direction	• Provider • Consumer Need to configure 2 ports

Cluster

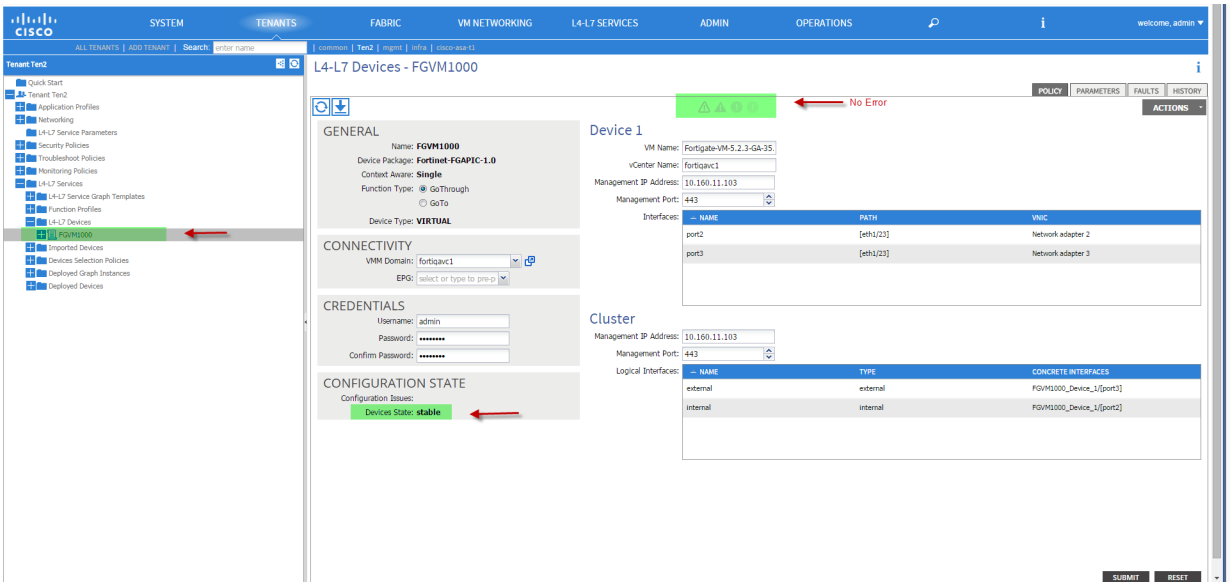
Leave everything default.



No need to input any information for next screen, just hit “submit”.



L4-L7 Device Added:



There are a number of steps that follow such as:

- Creating a Tenant
- Creating an Application Profile
- Creating an Application End Point Group (EPG)
- Creating Contracts

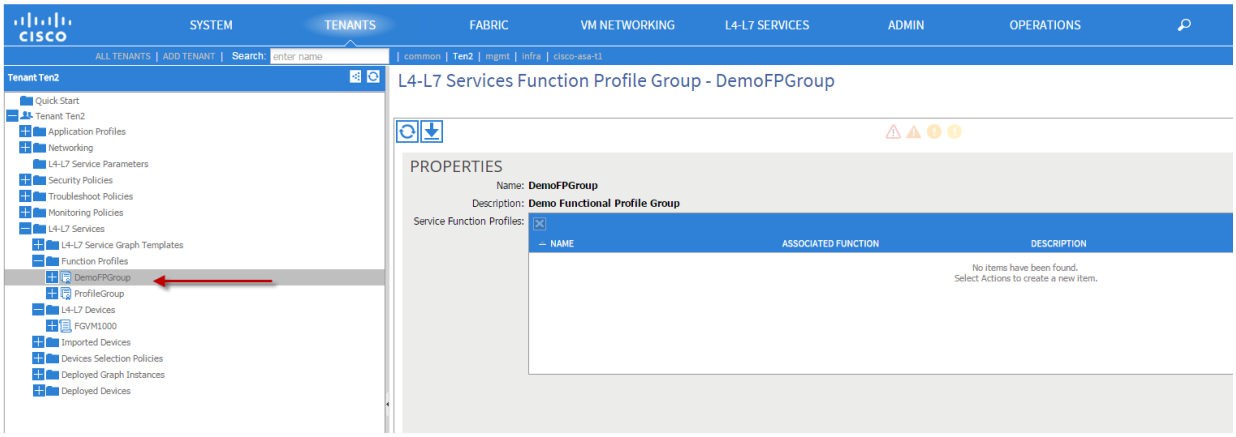
- Associate Physical Domains
- Assign Client to EPG (Static Bindings)
- Associating Contracts
- Associate the Device Package with the Tenant
- Deploy the Device

The instructions for these steps can be found in the Cisco Documentation at http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/L4-L7_Services_Deployment/guide/b_L4L7_Deploy.html

Create a Function Profile

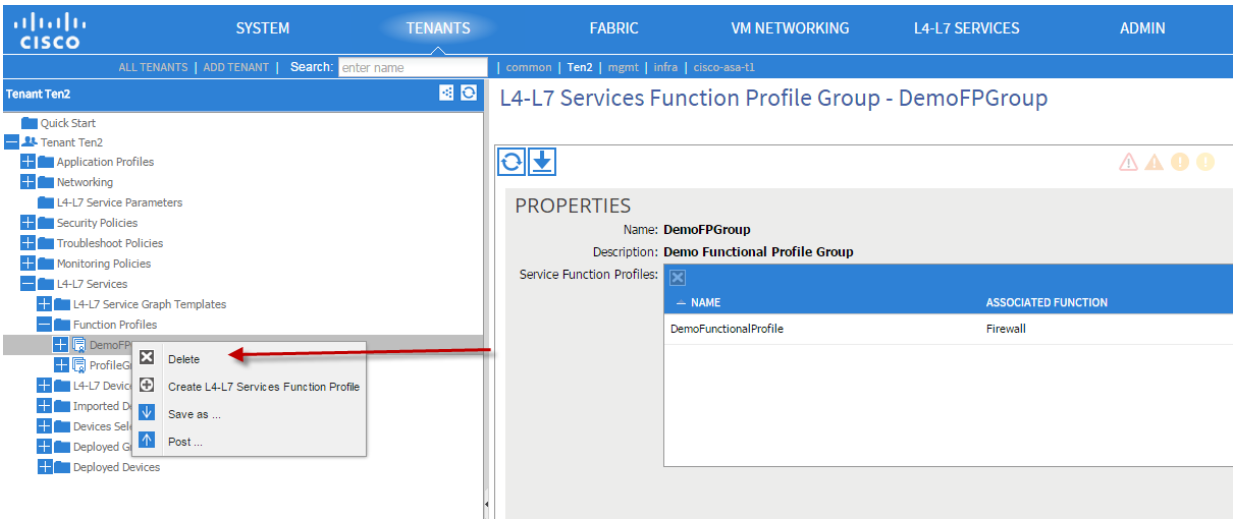
Functional Profile defines the template for the Service(s) that is going to deploy such as L4-L7 Device Interface IP addresses, Rule ID, Object Addresses, Policy Rules, Source/Destination Ports…etc.

Create Functional Profile Group



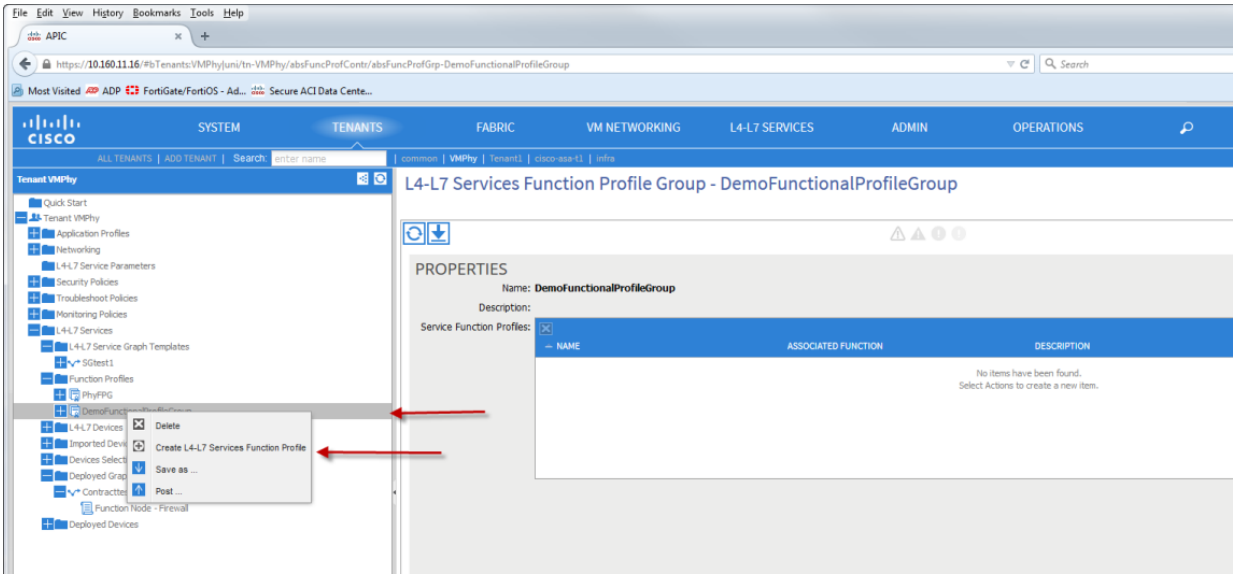
Remove Functional Profile Group

To remove Functional Profile Group, navigate to ***Tenant > L4-L7 Services > Functional Profiles*** and right click on the Functional Profile group name listed on the left hand panel and select ***Delete*** option.

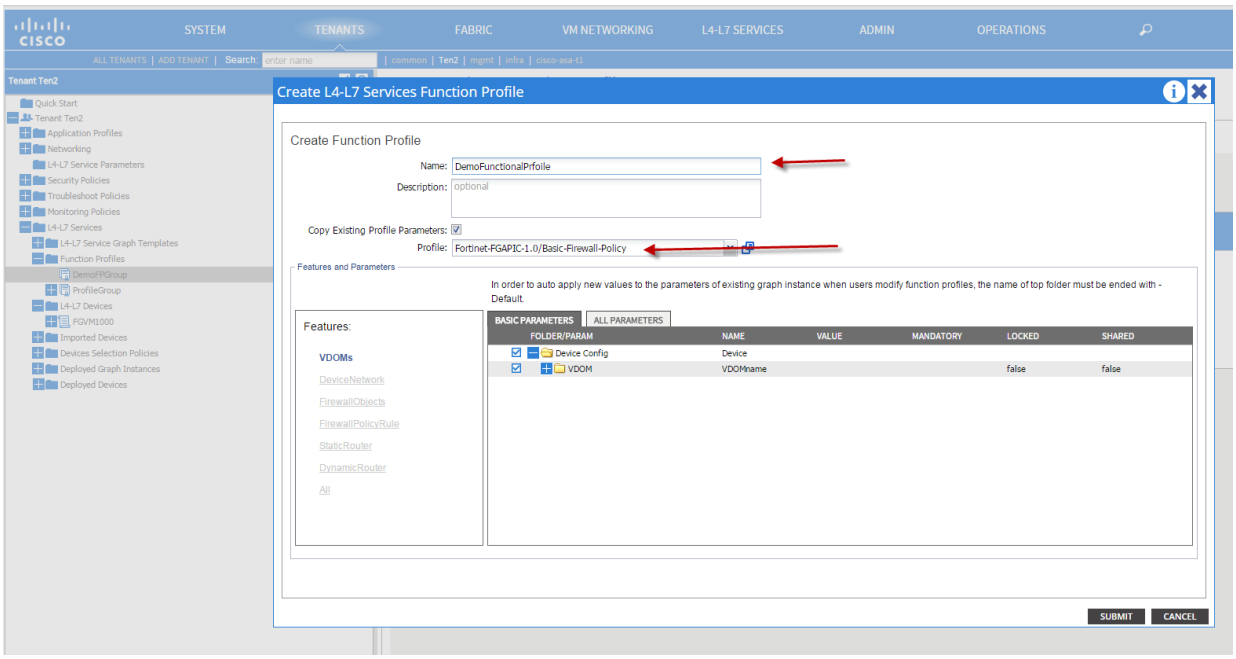


Create Functional Profile

1. Navigate under ***Functional Profile*** group created from above right click and select ***Create L4-L7 Service Functional Profile***

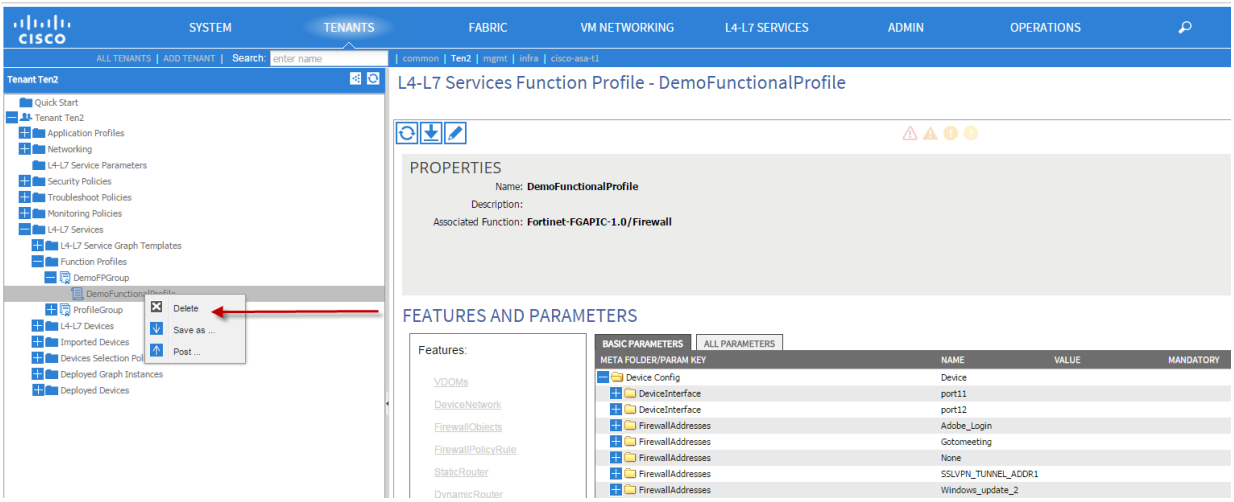


2. Input Functional Profile Name, and leave ***Copy Existing Profile Parameters*** option checked and select Profile: Fortinet-FGAPIC-1.0/Basic-Firewall-Policy



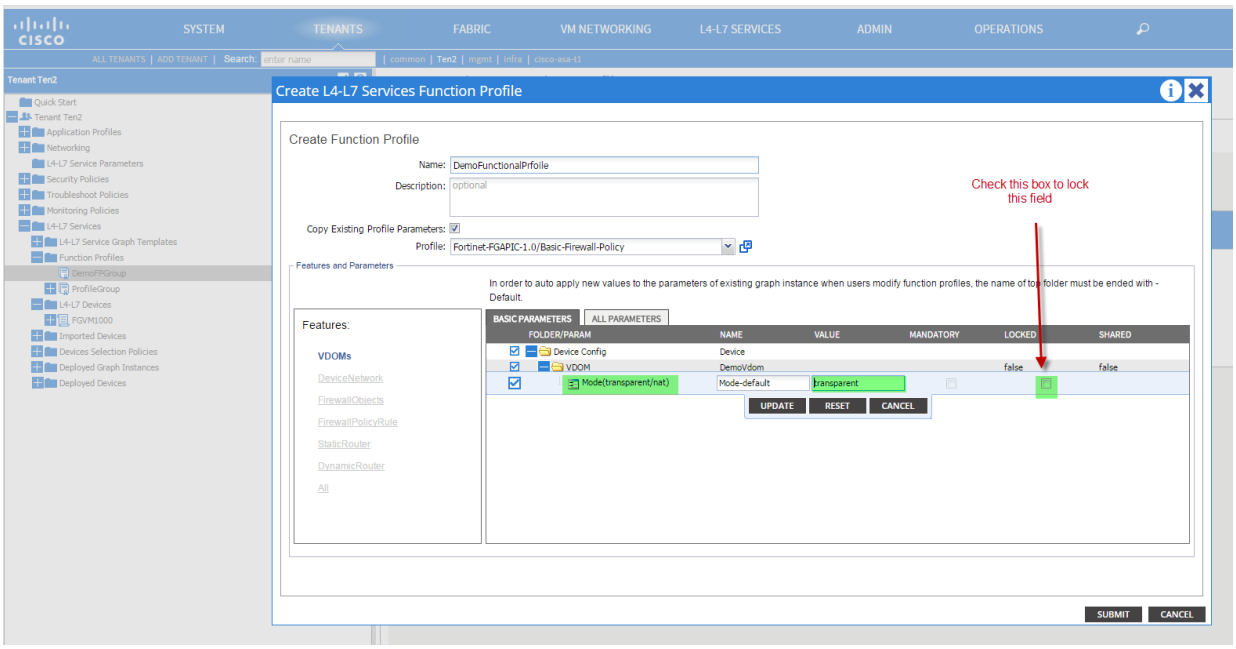
Remove Functional Profile

To remove Functional Profile, navigate to ***Tenant > L4-L7 Services > Functional Profiles*** > profile name listed on the left hand panel and select ***Delete*** option.



VDOMs

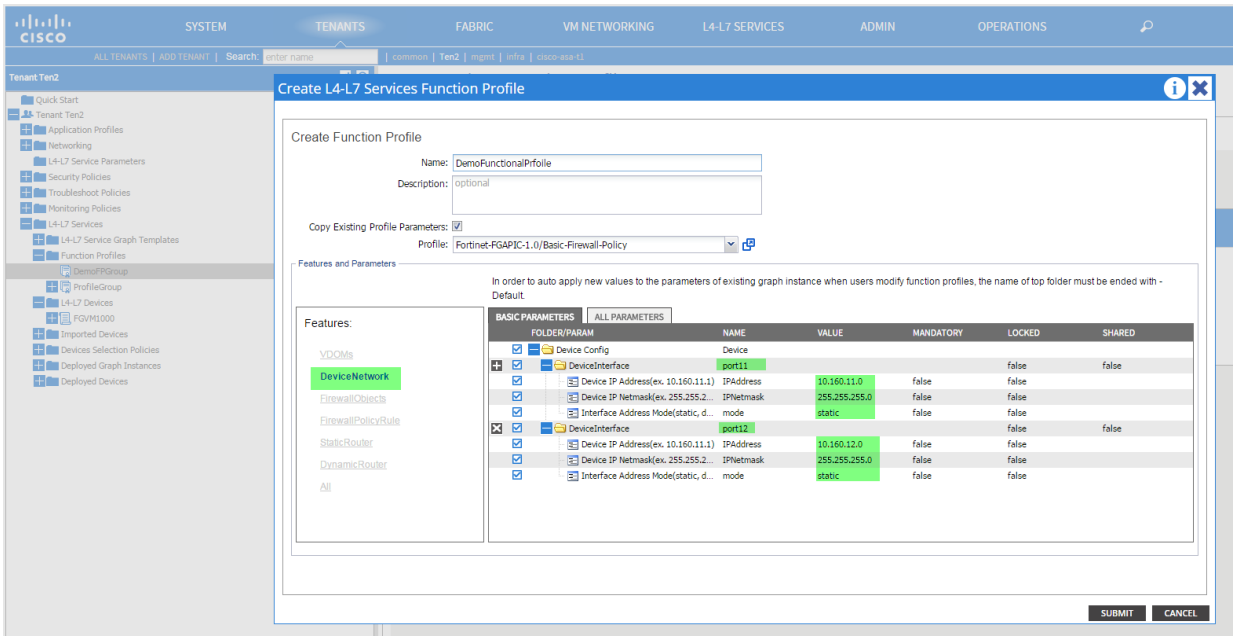
1. Input Vdom Name under the Name Column and check the box under Locked column.
2. The Locked column is used to lock the field to ensure you can not make any modification after the deployment of the service graph. In this case, we do not want to change the mode of the VDOM from L2 to L3 or vice versa. This is a limitation for the moment since changing the VDOM mode requires removal of the original VDOM deployment and re-deploy with the new mode.



Device Network

Device Network is defining the physical interface information. For transparent mode, it is not required therefore you can input dummy information into the field. All the fields are following the same layout as what is seem from Fortigate interface.

Default populated port name are “port11” and “port12”, please make the changes accordingly by double clicking on the name field. Rest of the fields highlighted in green from below need to be update.

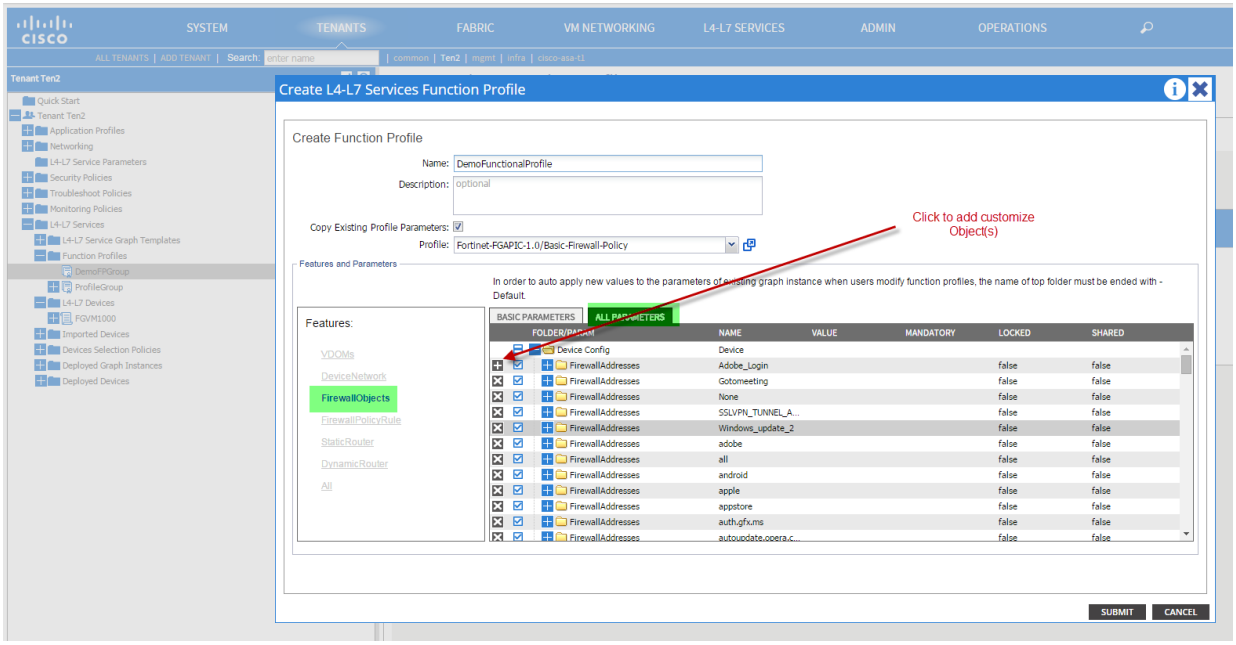


Firewall Objects

Firewall Objects field is pre-populated with default Objects from FortiGate. Please note that you need to select the “All Parameters” field in order to see the full list of default Objects. If you want to customize object(s), click on the + icon to add Object(s), otherwise, just move on to the next featured.

Firewall objects include Address object, Service object and Schedule object. These objects can be used in policy rule. For this release, the service object supports TCP, UDP, SCTP ICMP and IP only.

The screen shot below helps explain the customized Firewall Service.

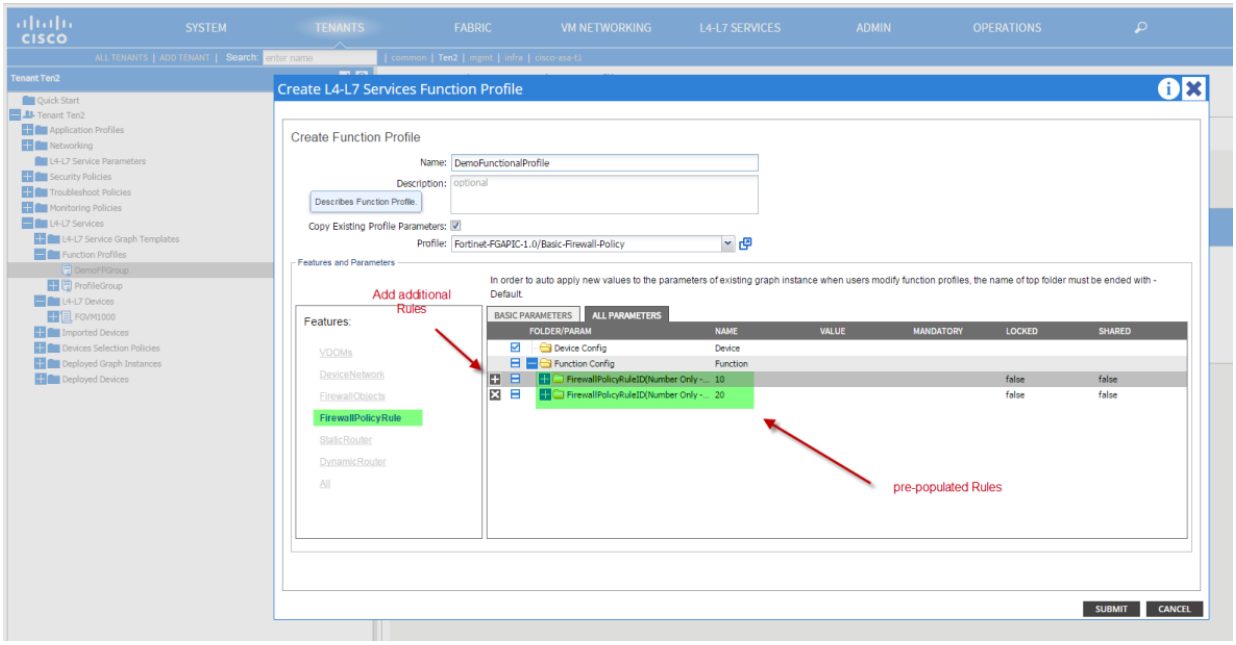


Field	Description
Firewall Service Field	Enter the name for the Firewall Service
Port Range	If you have more port range to define then click on the left hand “+” icon to add additional Port Range Field.
Dst/Src Port for TCP/UDP/SCTP	Select from drop down list to select your protocol. “TCP”, “UDP” or “SCTP”
TCP/UDP/SCP – Dst Port Range Max [0-65535]	Upper range of the Destination port range
TCP/UDP/SCP – Dst Port Range Min [0-65535]	Lower range of the Destination port range
TCP/UDP/SCP – Src Port Range Max [0-65535]	Upper range of the Source port range

Field	Description
TCP/UDP/SCP – Src Port Range Min [0-65535]	Lower range of the Source port range
Category	Select from the drop down list to select your Category
ICMP –code [0-255]	Part of the ICMP entry if your service is relating to ICMP
ICMP –port [0-255]	Part of the ICMP entry if your service is relating to ICMP
IP – Protocol Number [0-254]	If the Service is relating to IP, this is where you define the protocol number if any
Protocol Type (TCP/UDP/SCP, ICMP, IP)	Select from drop down list the desire protocol type

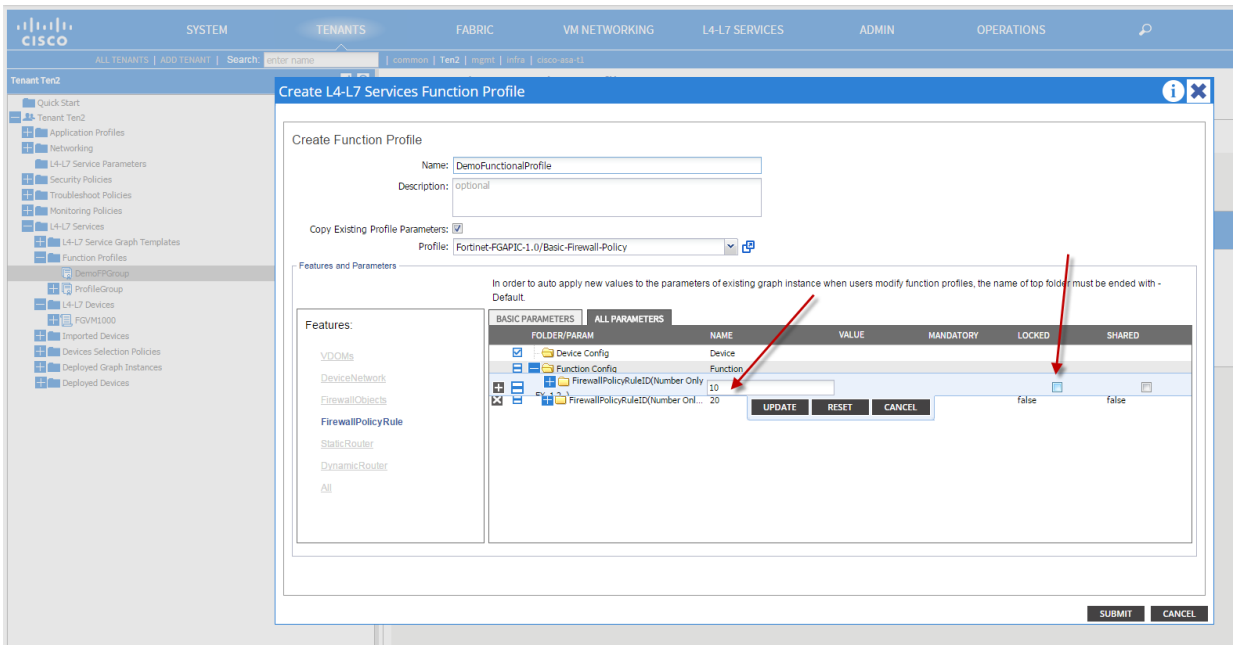
Firewall Policy Rule

Firewall Rule is where we define the Policies on Fortigate. There are 2 default rules pre-populated. You can modify the 2 default rules or add additional rules by clicking on the + icon.



Rule ID:

Rule ID defines the order how the rule will be applied later on to FortiGate. Lower Number Rule number will be listed first. The Locked icon is used to lock the field or any other field in the template so the modification cannot take place.

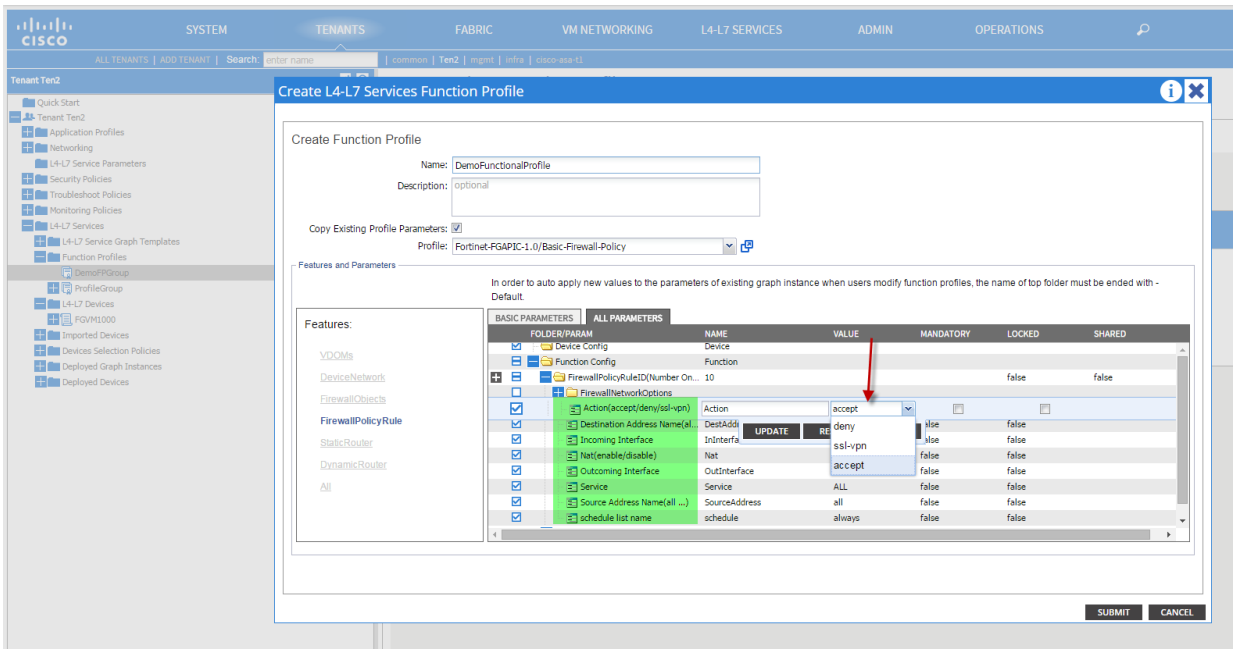


Rule Policy Fields

All the fields:

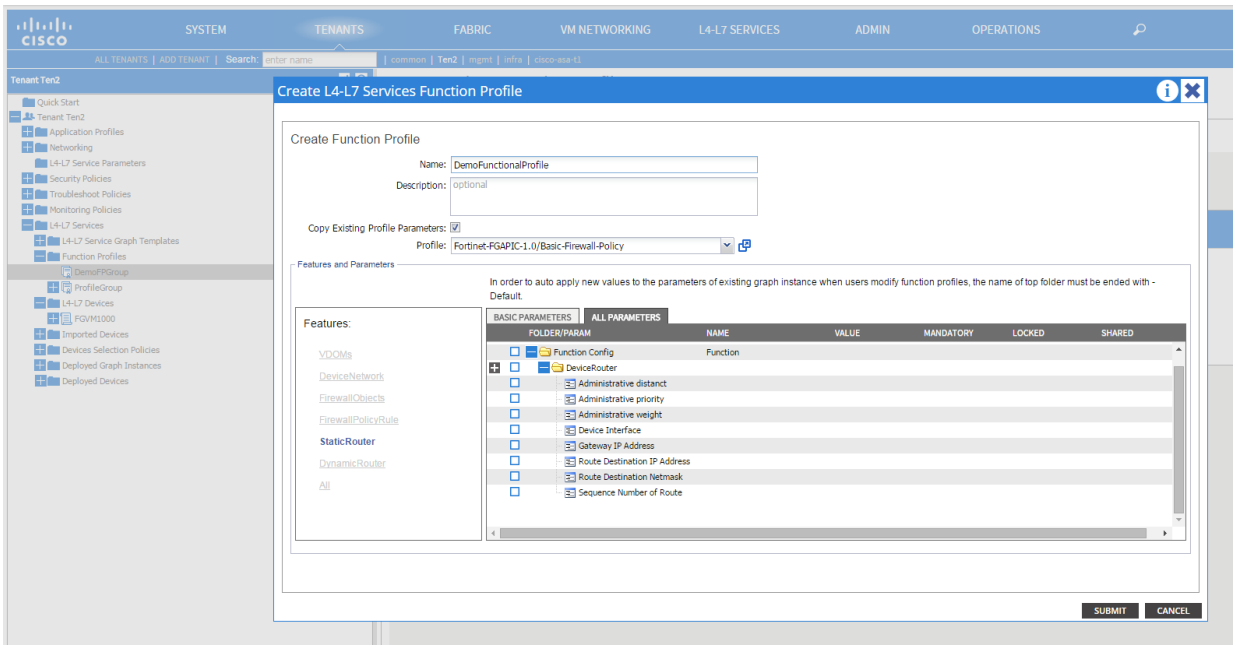
- Action
- Destination Address Name
- Incoming Interface
- NAT
- Outcoming Interface
- Service
- Source Address Name
- Schedule List Name

are pre-populated from basic template which you can select their value by select from the drop down menu under the Value column.



Static Router

For current release, we only support Static Route. You have to manual input all parameters for static route configuration.

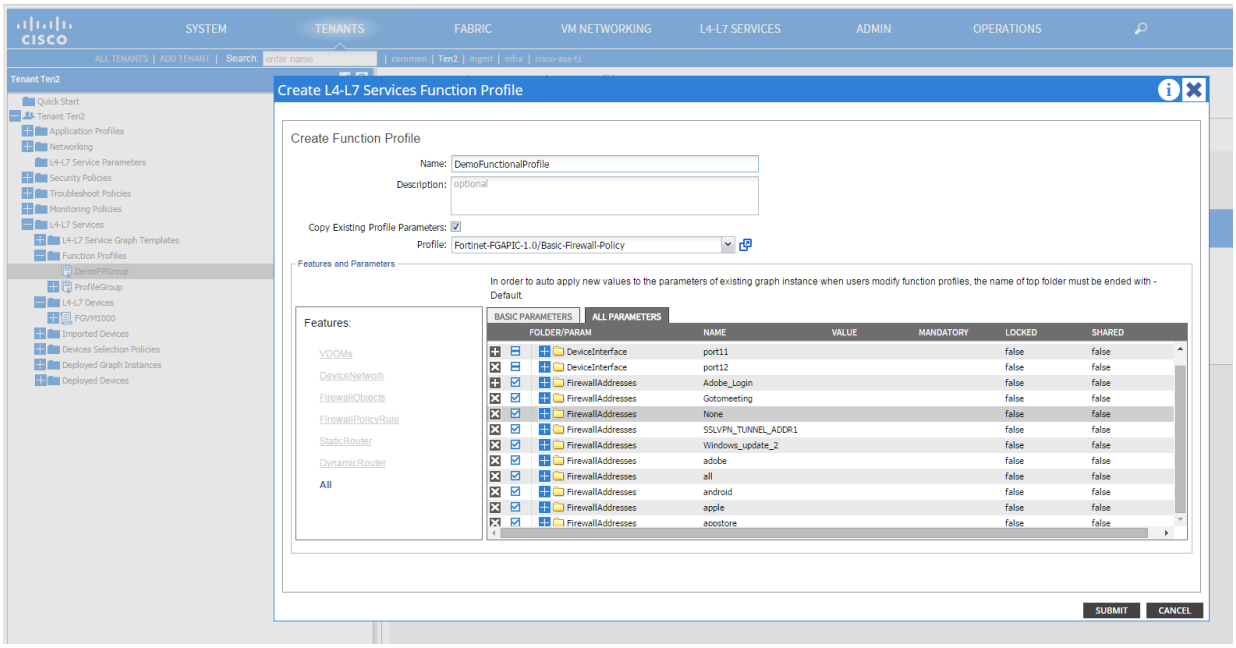


Dynamic Router

Not support for current release.

Review

All Field display all the fields in the features listing. If you are satisfy with all your inputs, then hit the submit button to complete your creation of Functional Profile template.

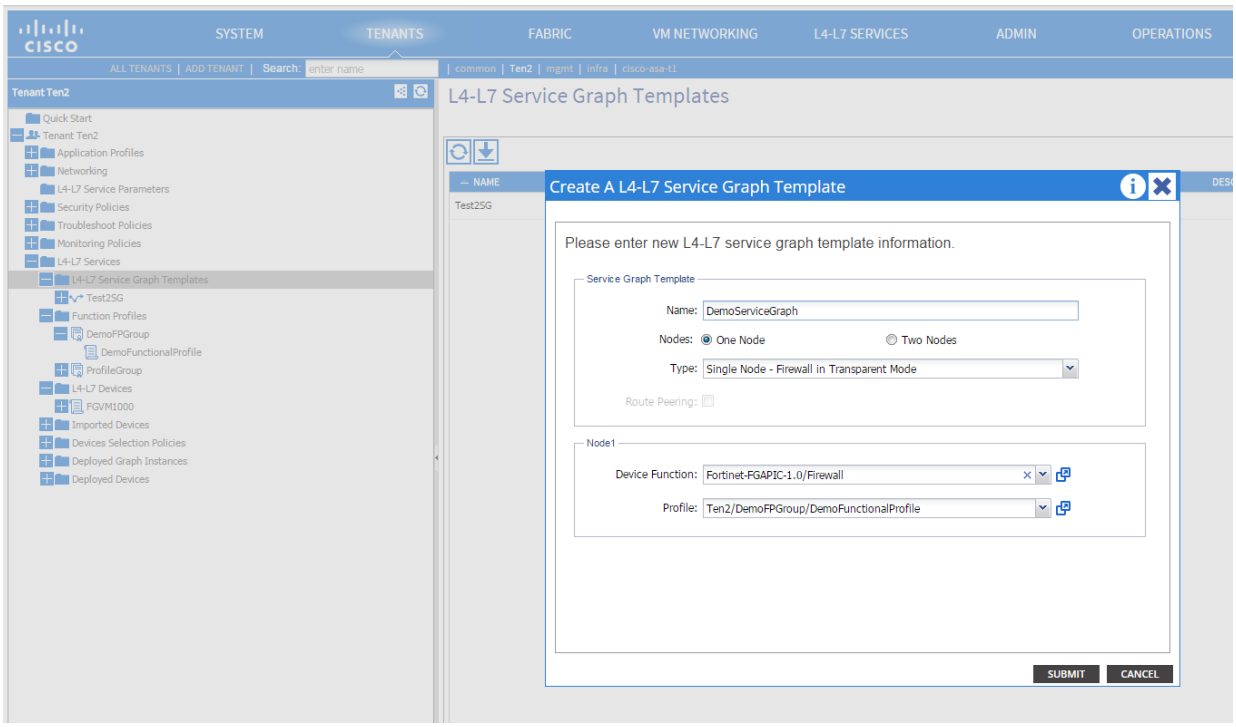


Service Graph

Create Service Graph

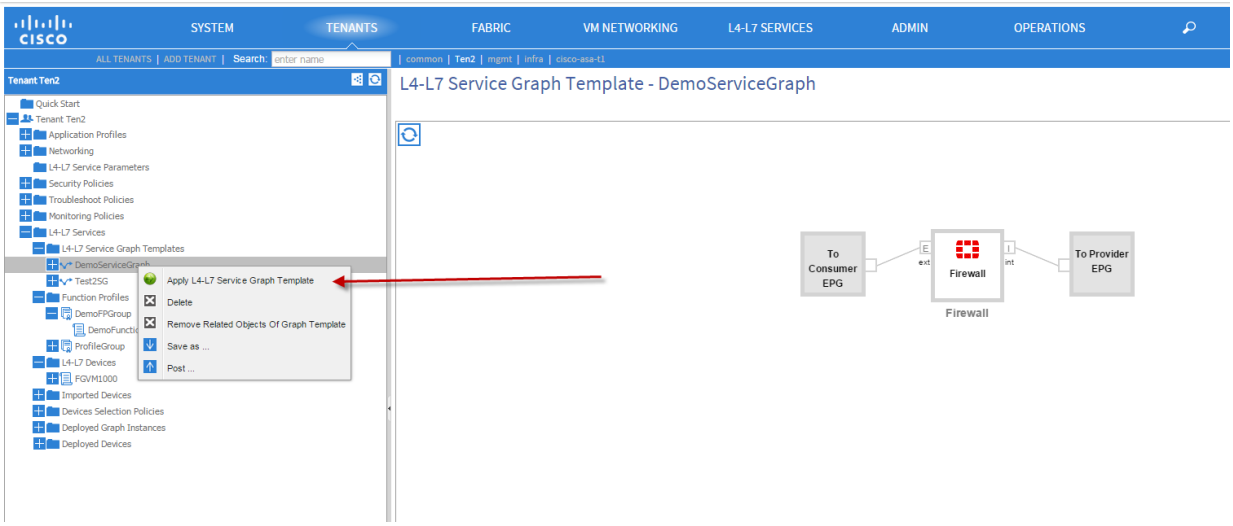
Right Click on ***L4-L7 Service Graph Template*** to create a Service Graph.

Field	Description / Options
Name	Name of the Service Graph
Node	• One node • Two node
Type	• Single Node Transparent • Routed In our case it is transparent
Device Function	Select the Device Package
Profile	Select the Functional Profile created earlier from the drop down list

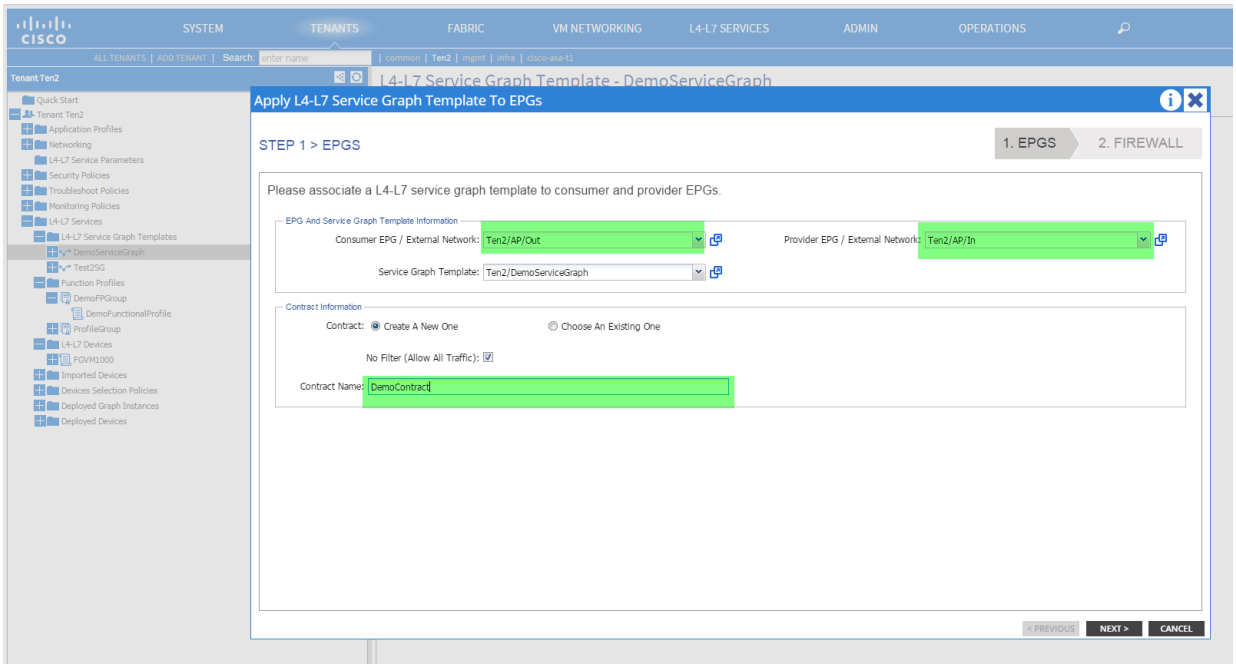


Deploy Service Graph

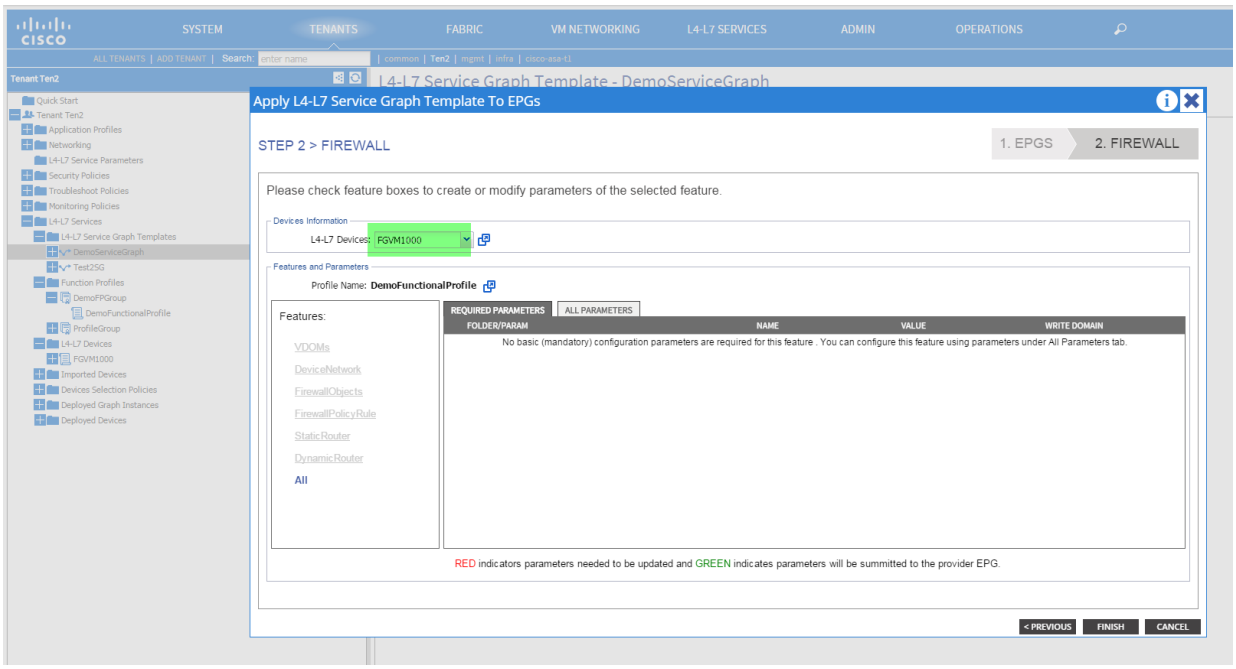
1. Right Click on Service Graph defined from above and select ***Apply L4-L7 Service Graph Template.***



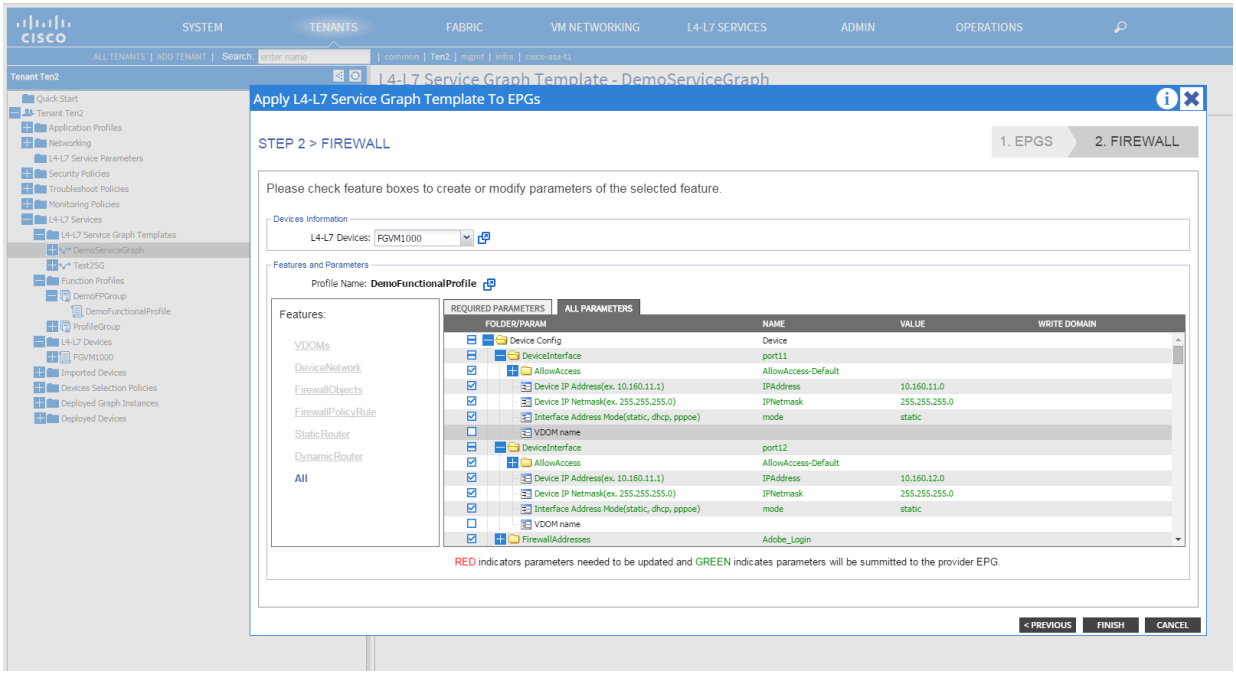
2. Select Consumer EPG and Provider EPG and input a contract name



3. Select L4-L7 Device

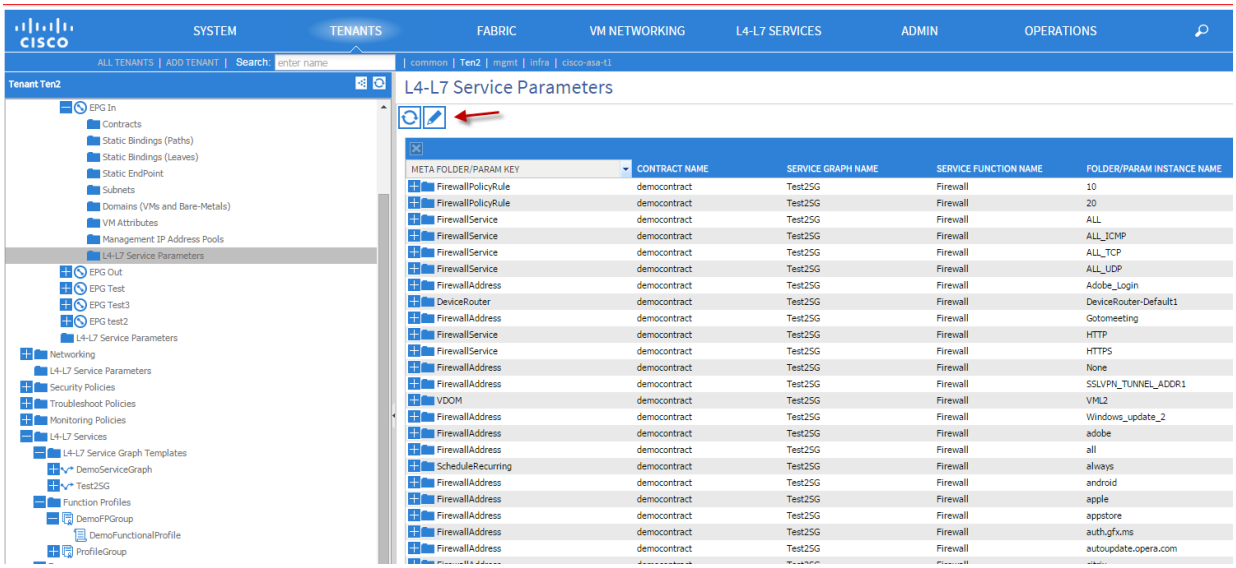


4. Ensure all fields turned Green, otherwise they will not get deploy/allow to modification later on. This is the last round of check before you hit to submit button to ensure everything is correct.

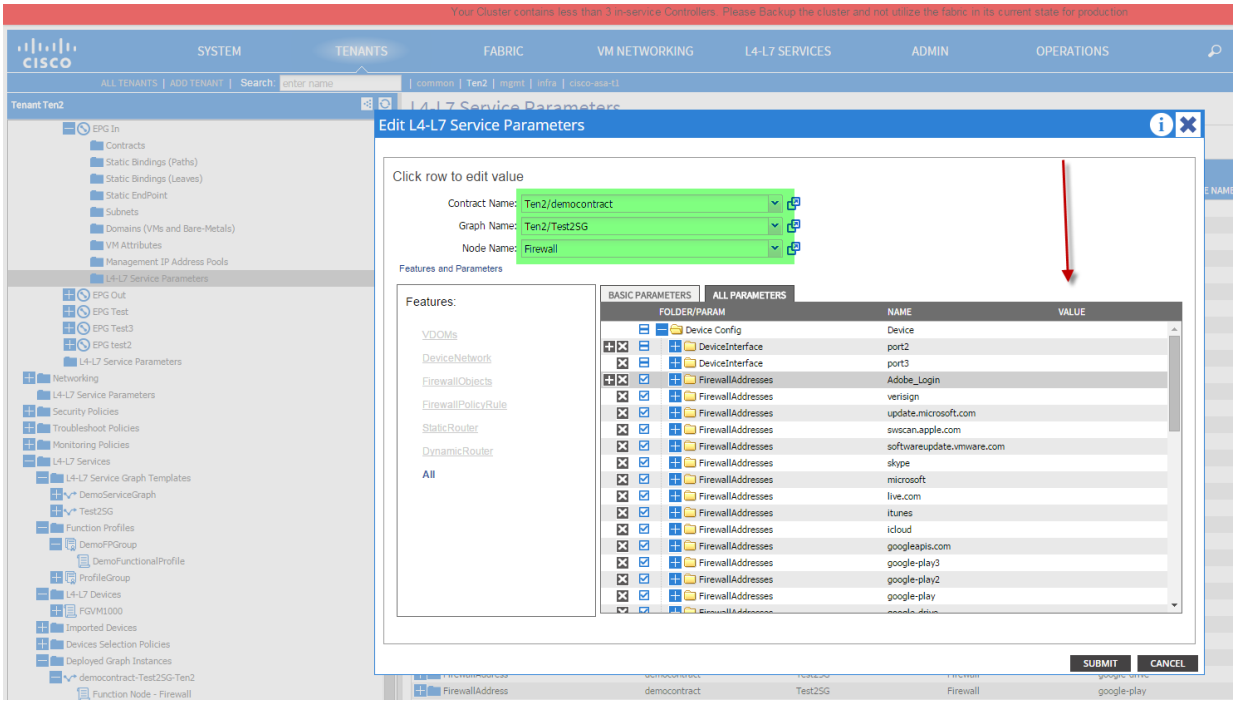


Modify Service Graph

1. Navigate to ***Tenant>Provider EPG>L4-L7 Service Parameters*** and select the pen icon.

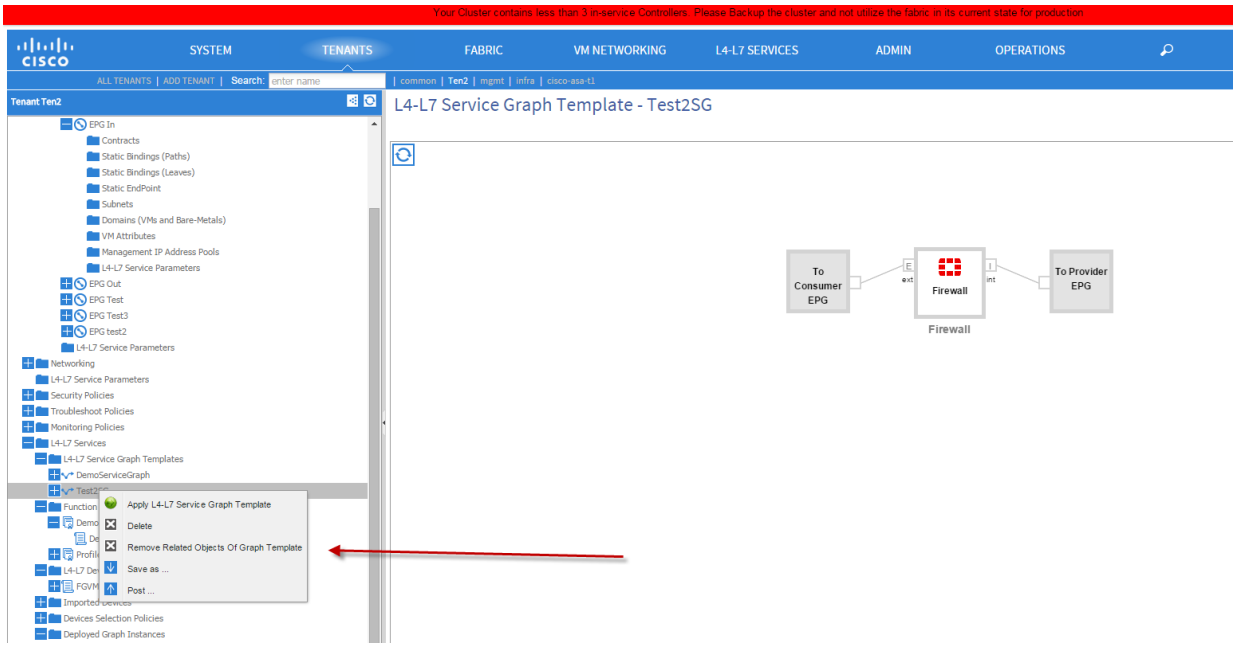


2. On the next screen, select the Contract name, Graph Name and Node name from the drop down list and all the associated Service Graph Parameters will be displayed.
3. Expand the field you want to make modification and change the appropriate value from the drop down list and then hit submit.



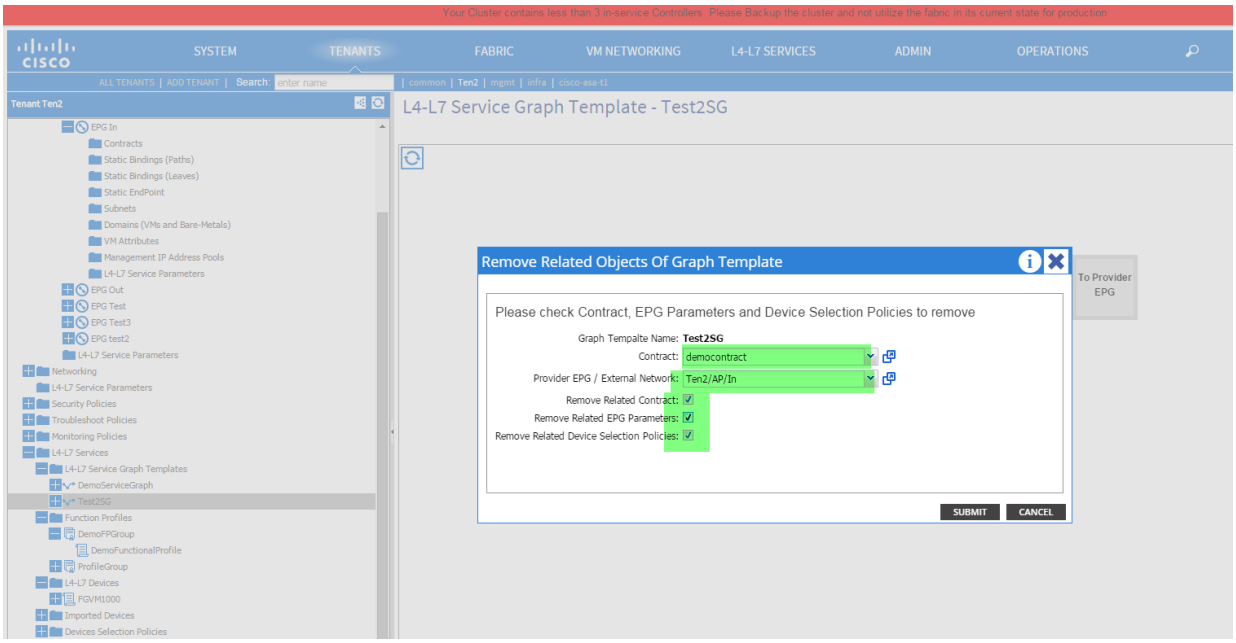
Remove Service Graph

1. Navigate to ***Tenant>L4-L7 Services>L4-L7 Service Graph Templates*** and the deployed Service Template name, right click and select ***Remove Related Objects Of Graph Template.***



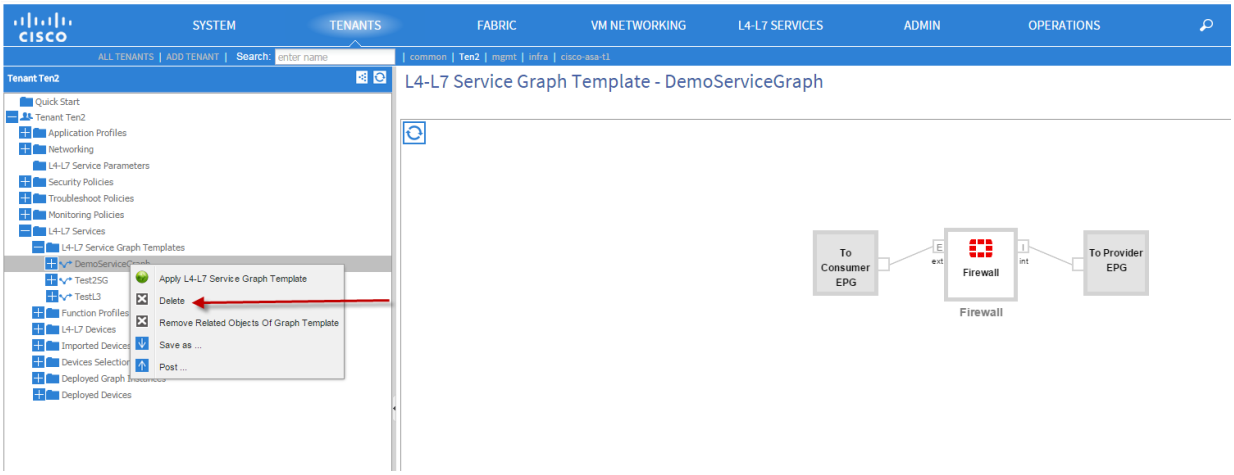
2. Select ***Contract and Provider EPG*** from the drop down list and check all 3 boxes:
   - ***Remove Related Contract***
   - ***Remove Related EPG Parameters***
   - ***Remove Related Device Selection Policies***

   Hit ***Submit***. This will remove all the related objects for this Service Graph.



Delete the Service Graph

1. To delete the Service Graph Template, navigate to ***Tenant > L4-L7 Services > L4-L7 Service Graph Templates***.
2. Right click on template name listed on the left hand panel and select ***Delete*** option.



APIC Infrastructure and FortiGate rollback

1. Upload and unload device package
2. Add and Delete device, FortiGate should clean-up previous configuration.
3. Dynamically modify and update policies
4. Detach and Attach service graphs
5. Delete tenants while service graphs in use.

Basic Troubleshooting

Verify Service Graph deployed

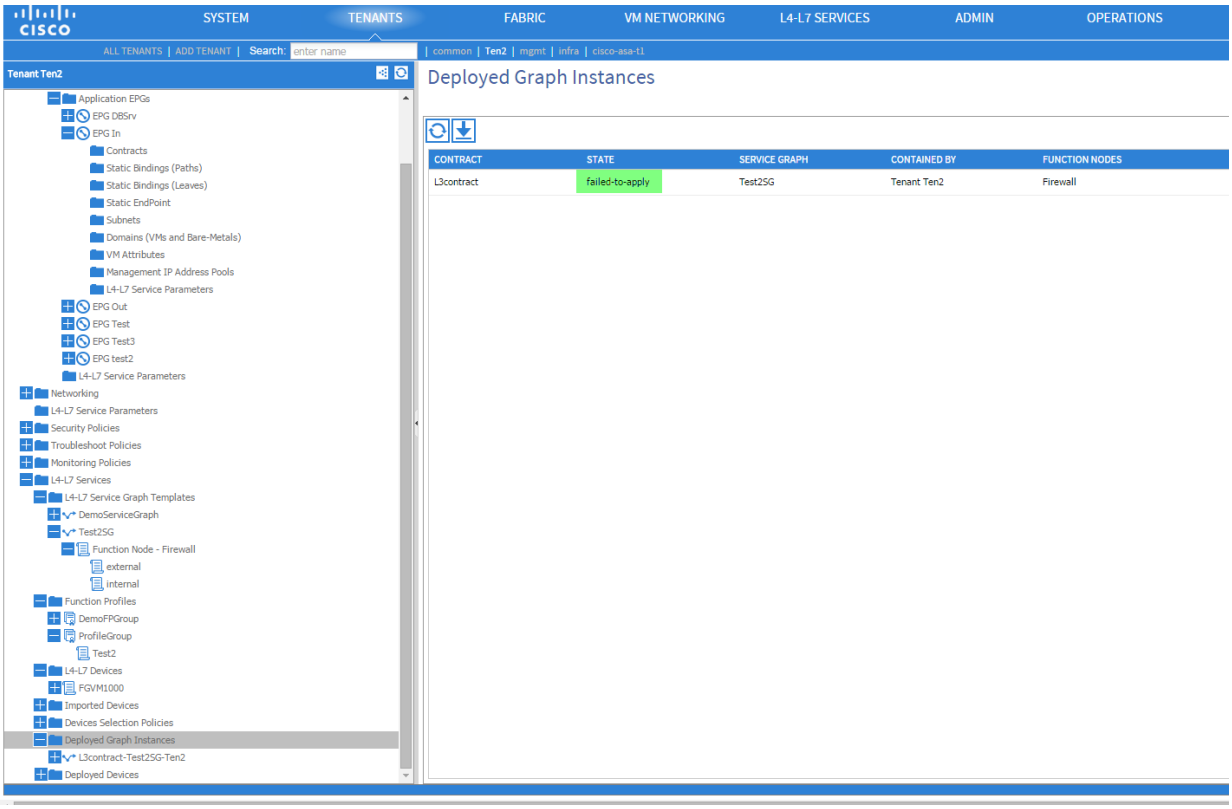
If Service Graph Deployed failed:

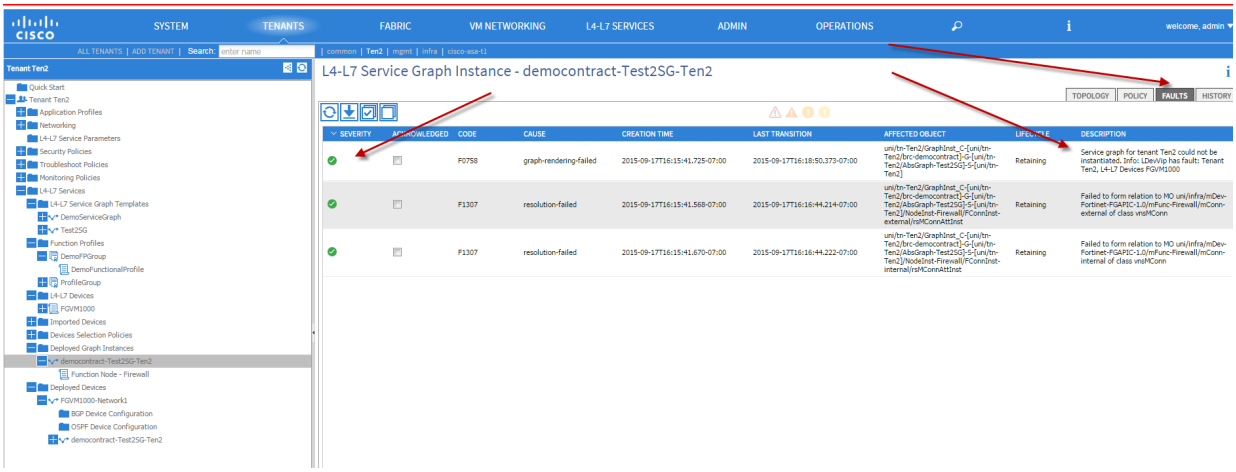
Navigate under ***Tenant > Deployed Graph Instances*** to check the state of the deployed graph.

If state is ***failed apply***, then go down one level to the ***Deployed Graph Instances*** and navigate to the ***Fault*** tab to check the error log. Any error code in 1000 range are relating to FortiGate while others belong to APIC

Currently we only have the following error code:

Error Code	Definition
1010	Configuration Error in device configuration
1020	Configuration Error in function configuration
1030	Internal Error -3
1040	Internal Error -4
1050	Internal Error -5
1070	Feature not available





Service deployed but parameters missing

If Service deployed but certain parameters not showing up on Fortigate, please follow the below steps:

1. Navigate to ***Tenant> Provider EPG>L4-L7 Parameters***, ensure the missing parameters are listed.If not, double check the functional profile to confirm the configuration

.

2. If yes, login on to Cisco APIC controller to examine the debug log. The debug log is located at `/data/devicescript/Fortinet.FGAPIC.1.0/logs` and the log file name is `debug.log`. Examine the log file and grab fields with "`[10.160.11.103, <xxxx>]:`" formats and scan through the logs associated to the parameters in question.
3. If all failed, please forward the entire captured log to Fortinet Technical Assistance Center for further troubleshooting.